Dynamic and Automatic Connection of Personal Area Networks to the Global Internet

Rui Campos
Fac. Eng. Univ. of Porto and INESC Porto
Rua Dr. Roberto Frias, 378
4200-465 Porto, Portugal
rcampos@inescporto.pt

Manuel Ricardo
Fac. Eng. Univ. of Porto and INESC Porto
Rua Dr. Roberto Frias, 378
4200-465 Porto, Portugal
mricardo@inescporto.pt

ABSTRACT
In the Next Generation Networks (NGNs) users will carry multiple devices forming cooperative networks known as Personal Area Networks (PANs). Some existing technologies enable this type of networks, such as Bluetooth or IEEE 802.15.4, but a unified framework capable of self-organizing them dynamically in a full heterogeneous environment populated by these and other technologies still has to be defined. Also, these networks are envisioned to be connecting dynamically to the Internet, and may use two IP versions and their autoconfiguration mechanisms.

In this paper we propose a new framework, the Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which enables the automatic and dynamic deployment of PANs in the heterogeneous environments envisioned for NGNs and handles the automatic and dynamic connection of a PAN to the global Internet.

Categories and Subject Descriptors
C.2.1 [**Computer – Communication Networks**]: Network Architecture and Design – *Network communications, Packet-switching networks, wireless communications*.

General Terms
Management, Design, Theory.

Keywords
Personal Area Networks, Dynamic Autoconfiguration, Self-management, Ubiquitous Connectivity.

1. INTRODUCTION
Next Generation Networks will be characterized by a movement towards ubiquitous connectivity. This includes an increasing number of wireless and wired technologies, multi-homed devices, and mobility of networks and end-users. In this communication scenario, user intervention must be minimized and technology must seamlessly adapt to different networking contexts and user needs. The increasing number of devices expected to be carried by a person, combined with the integration of electronic devices having computing and communications capabilities within clothes, human environments, or even in the human body, will trigger the emergence of new computing environments and bring up new communication models; some of these devices will form cooperative networks, such as PANs. It becomes consensual that IP will be the base protocol for NGNs; Internet will play a central role, supporting multimedia data and services, from the classical such as web browsing and e-mail, to more QoS demanding services such as VoIP or video-conferencing; it will be the network to which most of the devices need to be connected.

Nowadays, small incipient cooperative networks such as Bluetooth [3] PANs can be created. However, they require manual configurations and networking expertise. Furthermore, Bluetooth does not provide mechanisms to adapt automatically to scenarios where, for instance, a PAN is changing its point of attachment (PoA) to the Internet dynamically; other solutions, namely IEEE 802.15.4 [7], are proposed for creating PANs but they care only about creating a PAN at the data link layer. On the other hand, IP networks are also becoming heterogeneous; different protocol suites operating simultaneously (IPv4, IPv6), and multiple addressing schemes (private IPv4, public IPv4, IPv6) and autoconfiguration mechanisms can be used. In addition, new autoconfiguration frameworks, apart from those already defined in IP networks, e.g., DHCP [13], will be required for scenarios where an entire network connects to the Internet while moving. In this context, enabling the automatic and dynamic creation of PANs, and dealing with its dynamic and automatic connection to the global Internet poses new requirements to mobile communication systems, namely in terms of autoconfiguration and self-management.

Intensive research on this field is being carried out. Ongoing research projects and multiple discussion forums address these topics, and point out solutions; in [9,11,15] such solutions are presented. Nevertheless, to the best of our knowledge, no solution tackles simultaneously the integration of multiple wireless and wired technologies, the IP heterogeneities aforementioned, and the self-organization and automatic and dynamic connection of PANs to the global Internet in these heterogeneous environments.

In this paper we present a new framework, the Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which addresses this problem. ASPAN can negotiate the proper IP version and autoconfiguration mechanism to be used within a PAN, taking into account the characteristics of the PAN devices and the characteristics of their PoAs towards the Internet. Additionally, it defines mechanisms for self-creating and self-managing a PAN in these heterogeneous environments, and deals with the dynamic and automatic connection of a PAN to the Internet based on user-defined policies.

IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada.

The rest of this paper is organized as follows. Section 2 presents the state of the art on autoconfiguration in IP networks and personal area networks. Section 3 presents the problem. Section 4 describes the ASPAN framework and, finally, Section 5 draws the conclusions.

2. STATE OF THE ART

We characterize the state of the art from two perspectives: autoconfiguration in IP networks and Personal Area Networking.

2.1 Autoconfiguration in IP Networks

Autoconfiguration mechanisms in IP networks can be classified in two categories: stateful and stateless autoconfiguration. Herein, we mention the most typical mechanisms; in [11] other standard mechanisms are described.

The Dynamic Host Configuration Protocol (DHCP) [13] provides a framework for passing configuration information to hosts, using a client/server model. The client broadcasts a *DHCPDISCOVER* message in order to discover available servers; it may receive one or more *DHCPOFFER* messages and, after selecting one of the servers, it broadcasts a *DHCPREQUEST* containing the identification of the selected server. Finally, the server replies with a *DHCPACK* message containing the assigned address and optional information, such as DNS server address. With the advent of IPv6 DHCPv6 [14] came up, considering a different operation model: 1) a well-known multicast address is used by clients to address all the servers in the link, instead of broadcasts; 2) unlike DHCPv4, which is used to perform the whole host configuration, DHCPv6 can be used to just complement the stateless mechanism; 3) the messages defined for DHCPv6 are different in name and format. In real implementations, DHCPv4 and DHCPv6 are used independently for dual-stack hosts; possible solutions to integrate the two frameworks are suggested in [18].

The Dynamic Autoconfiguration of IPv4 Link-Local Addresses [16] is currently implemented by multiple operating systems, such as Windows XP and Linux, as an alternative to DHCP. In this solution a host can automatically configure an IPv4 address within the 169.254/16 prefix, which can be used for communicating with other devices in the same logical link. First, the host generates a random IP address using the 169.254/16 prefix. Next, it performs the duplicate address detection (DAD) using an Address Resolution Protocol (ARP) probe, in order to assess if the address is already in use; if a reply is received, it must consider that the address is being used by other terminal and must try a new address. Finally, the host assigns the IP address to the local network interface, and link local connectivity becomes possible.

The IPv6 Stateless Autoconfiguration mechanism [17] defines the steps carried out by a host to autoconfigure its network interfaces without using a centralized service. The autoconfiguration process comprises the generation of a link-local and a global address, and a DAD procedure in order to verify the uniqueness of the autoconfigured addresses. The autoconfiguration of a link-local address is performed upon network interface activation, and after combining the well-known prefix FE80::0/10 with the interface identifier (ID), based on the MAC address; configuration of a global address is accomplished by combining the prefix announced by a local router, using the Router Advertisement (RA) messages defined in [19], with the interface ID; optional information can be acquired using DHCPv6.

2.2 Wireless Personal Area Networks

Bluetooth [3] has become the de-facto standard for PANs. This fact may be even consolidated in the future since Bluetooth may adopt the ultra-wideband (UWB) technology; UWB may increase data rate by two orders of magnitude (i.e., from 1 Mbit/s to 100 Mbit/s), and enable the appearance of new Bluetooth applications such as real-time video. Bluetooth defines a set of profiles aimed at being used for different applications, such as transfer of a stereo audio stream and file transfer. Nonetheless, the relevant profile from Personal Area Networking standpoint is the so-called PAN profile. This profile enables the creation of Bluetooth-based PANs by providing Ethernet emulation over Bluetooth. In this sense, unmodified Ethernet payloads can be transmitted between Bluetooth devices using the Bluetooth Network Encapsulation Protocol (BNEP) and the deployment of IP networks over Bluetooth becomes easier.

The PAN profile defines the formation of a PAN in the following situations: (1) ad-hoc IP networking by two or more Bluetooth devices in a single piconet[1]; (2) external network access for one or more Bluetooth devices. Each Bluetooth device may implement one of the following services: PAN User (PANU), Gateway Node (GN), or Network Access Point (NAP). The profile specifies three scenarios: Network Access Points, Group Ad-hoc Networks, and PAN User to PAN User. In the first scenario there is a node deploying the NAP service which is able to provide access to some external network, such as Ethernet or cellular network; this device acts as a bridge or router between the Bluetooth PAN and the external network; the other devices connect to it as PANUs. In the second scenario, Group Ad-hoc Networks, devices cooperate to create a stand-alone PAN; one of the devices acts as the master and implements the GN service; the other devices are slaves and are connected to the master as PANUs. The third scenario provides a point-to-point connection between two PANUs and enables direct communication between them only; this scenario is equivalent of connecting two devices using an Ethernet cross-over cable. The PAN profile specifies IP as its major internetworking protocol. Apart from the Bluetooth features, the specification provides the Request For Comments (RFCs), the address assignment, and the name resolution techniques required to enable IP over Bluetooth. The address assignment for IPv4 is based on the Dynamic Configuration of IPv4 link-local addresses mechanism; for IPv6, the IPv6 stateless autoconfiguration mechanism must be supported.

In the scope of the Institute of Electrical and Electronic Engineers (IEEE), the IEEE 802.15 Working Group for Wireless PAN (WPAN) [7] is developing standards for PANs or short distance wireless networks. These WPANs address wireless networking of portable and mobile computing devices such as laptops, Personal Digital Assistants (PDAs), peripherals and mobile phones at the data link layer. This work group has been partitioned in Task Groups (TGs) which address specific sub-areas within the Personal Area Networking area. The IEEE 802.15.1 Task Group (TG1) has reviewed and provided a standard adaptation of the

[1] Network where one Bluetooth device operates as the master communicating with up to 7 active Bluetooth devices operating as slaves

Bluetooth Specification version 1.1 for the Medium Access Control (MAC) and physical layers. The IEEE 802.15.3 (TG3) has provided a standard for high data rate and is currently working on enhancements to that standard in order to reach data rates up 600 Mbit/s, whereas the IEEE 802.15.4 (TG4) is chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity, whose potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.

Solutions concerning IP-based PANs have been proposed along the last few years. In [5] the deployment of IP-based PANs using Mobile Ad-hoc Networks (MANET) technologies and a so-called PAN middleware that presents the PAN as a virtual device to the user and applications is defined. However, this approach does not address, for instance, the heterogeneities found in current IP networks; on the other hand, the definition of the PAN middleware represents a disadvantage from legacy applications standpoint, as they have to be modified to take advantage of the new solution. Other solutions concerning WPANs, IP-based PANs and Internet access for MANETs are referred in [9,11,15]. Nevertheless, to the best of our knowledge, no existing solution addresses the problem undertaken herein; the deployment of IP-based PANs in the heterogeneous environments of NGNs, the dynamic and automatic connection of a PAN to the Internet, by using different PAN devices, and the selection of the best access network, by taking into account user policies dynamically defined, are aspects not fully considered by existing solutions.

3. PROBLEM STATEMENT

Currently a person carries a set of terminals. A common scenario is to have persons carrying devices with communication capabilities, which cooperate loosely, or do not cooperate at all. For instance, the user utilizes her mobile phone to make phone calls and send SMSs, the PDA as an electronic agenda, and the laptop as the major device to perform more computing demanding work. In spite of this, the creation of incipient PANs is currently possible, namely by using Bluetooth; the user utilizes her mobile phone to provide Internet access to her laptop or to her PDA.

Fig. 1 illustrates a typical networking scenario for NGNs from the end-user viewpoint, where multiple devices around her form a PAN; this network shall be self-created and self-managed according to dynamic network contexts and user needs, so that the involvement of the user is limited. Three moments in time (1, 2, 3) are represented in the figure which demand reconfigurations within the PAN. At instant 1 just the laptop, mobile phone, and PDA form the PAN; at instant 3 the video camera and the home PC become integrated in the network. Fig. 1 also shows the PAN connecting to various access networks along the time. At instant 1 the PAN is connected through UMTS to the Internet, but at instant 2 it decides to start using the WLAN access, because it offers better bandwidth and lower costs. This simple but rich scenario illustrates the dynamics and the adaptation required for the PAN.

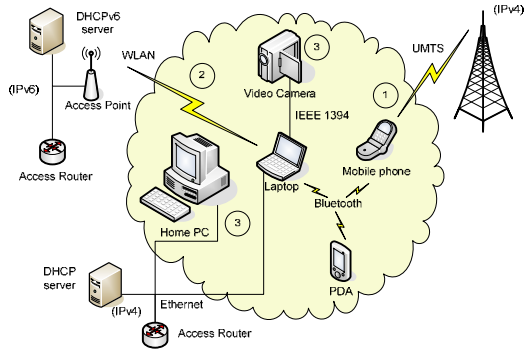

Fig. 1. Example scenario for NGNs from end-user perspective

The transition from a terminal-based to a network-based communication paradigm poses new requirements that are not addressed by legacy technologies. The solutions currently deployed and investigated for IP networks are mostly terminal-based. On the other hand, deploying PANs in the way mentioned is still impossible. The different technologies standardized in the context of the IEEE 802.15 work group, target Personal Area Networking scenarios, but do not address the dynamic and automatic connection of PANs to the global Internet, since they only address the MAC and physical layers. Also, the deployment of a Bluetooth PAN by using the PAN profile described in Subsection 2.2 is not a fully automatic process. In [11,12] is made an analysis of the shortcomings of the existing solutions.

4. ASPAN FRAMEWORK

In order to solve these problems we propose a new framework – the Autoconfiguration and Self-management of Personal Area Networks (ASPAN). ASPAN aims at being used in heterogeneous communication environments, where two IP versions and the corresponding autoconfiguration mechanisms coexist, and multiple wired and wireless technologies are defined. Two principles drive the ASPAN design: reuse the existing technology as much as possible, and no modification of the data plane. The first principle avoids the re-invention of the wheel and the second enables easier deployment of the new framework over legacy systems. ASPAN is a control plane framework working on behalf of the user and aimed at enabling ubiquitous IP connectivity. For that purpose it includes four major mechanisms:

- Mechanism for negotiating the IP version and the autoconfiguration framework to use in the PAN. It considers the communication characteristics of the PAN devices, and the PoAs available;
- Mechanism for automatic and dynamic selection of the best PoA towards the Internet based on user-defined policies and network context;
- Mechanism for configuring automatically and dynamically the PAN devices, according to the negotiations and selection performed by the previous mechanisms. E.g., configuration of a PAN device as a Network Address Translator (NAT);
- Mechanism for joining and leaving of PAN devices, including in multi-hop scenarios.

In the following subsections we present the architectural model of ASPAN and reason about the master-slave paradigm adopted. Then the advertisement/discovery, and the security issues are addressed. Finally, the join/leave mechanisms, somewhat similar to those defined in [1], the network configuration, and the intervention required by the user are discussed.

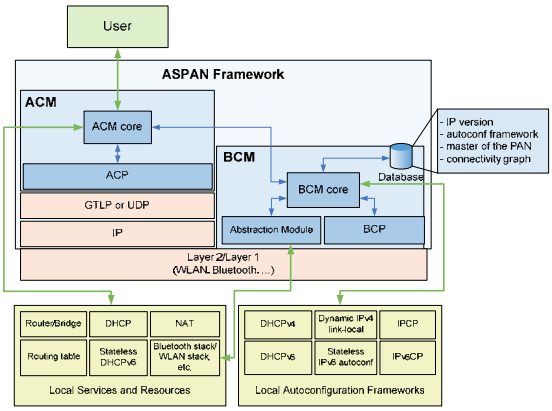

Fig. 2. Architectural model of the ASPAN framework

4.1 Architectural Model

The ASPAN framework includes two managers: the Basic Connectivity Manager (BCM) and the Advanced Connectivity Manager (ACM); Fig. 2 illustrates the architectural model chosen for the ASPAN framework.

The BCM deals with (1) the establishment of IP connectivity between the devices forming the heterogeneous PAN, (2) the selection of the autoconfiguration mechanism used to assign IP addresses and optional information to the PAN devices, (3) the join and leave of the PAN devices. BCM interacts with the local autoconfiguration frameworks, selects the mechanism negotiated a priori with peer BCM(s) using the Basic Connectivity Protocol (BCP), and enables/disables the proper protocol stack (IPv4, IPv6) according to the IP version negotiated with the peer BCMs. BCM also interacts with local services and resources; for instance, it selects the proper advertisement/discovery mechanism considering the layer 2 technologies available for communication (see Subsection 4.3). In addition, BCM interacts with ACM for informing the latter about the establishment of IP connectivity and the characteristics of the network interfaces created.

The ACM takes care of the dynamic connection of the PAN to the Internet, through the best PoA available; multi-homing is not, for now, being considered. The network context, the user-defined policies, and the configuration of local services and resources guide the behavior of ACM. Its interaction with local services and resources is shown in Fig. 2. ACM configures, for instance, a device to behave as a NAT/gateway towards the Internet, based on the connectivity service(s) negotiated with the other devices. The announcement of connectivity services, such as the PoA to the Internet, is performed using the Advanced Connectivity Protocol (ACP) between ACMs. The ACP protocol runs either on top of GANS Transport Layer Protocol (GTLP) or directly over UDP. GTLP is being specified in the Ambient Networks project [8,10], and it aims at transporting signaling information between Ambient Networks; it represents an extension to the General Internet Signaling Protocol (GIST) specified in [6].

4.2 Master-Slave Paradigm

A master-slave model was selected for ASPAN. When devices come together to form a PAN, one of them is elected as the master of the PAN through a distributed election algorithm. The device is elected master based on a set of parameters which include network interfaces characteristics, CPU, memory, and expected holding time. The master device manages the connectivity of the PAN, namely the detection of new PoAs and the detection of new devices willing to join the PAN. The information required for the master to take decisions comes from the other PAN devices, which act as slaves.

The set of devices forming a PAN have heterogeneous network interfaces and not every pair of devices may communicate directly. For that reason, the master maintains a graph modeling the PAN topology (see Fig. 3). We name this graph the *connectivity graph.* In this graph, a vertex represents a device and an edge represents a link (e.g., Bluetooth, WLAN) between two connected devices. This graph is similar to the information obtained using an IP routing protocol, but it also has some differences: 1) only the master builds it, not all PAN devices; 2) the graph enables the control of the PAN by the master; 3) the graph captures appropriately multiple PoAs towards the Internet, from the master's perspective. From the connectivity graph the master extracts a so-called *control tree* (drawn in bold in Fig. 3). The control tree allows the master to know how to reach each slave; each slave can reach the master through its parent node in the tree (e.g., in Fig. 3 *Slave3* can reach the master through the sub-master – its parent node). The connectivity graph is dynamic and depends on the number of devices in the PAN. The connectivity graph is stored in the database represented in Fig. 2, inside the BCM.

A pure master-slave model creates a single point of failure: if the master leaves the PAN, a new PAN would have to be created from the scratch. In order to overcome this problem, a sub-master is also elected during the master election process; this sub-master mirrors the control data required to maintain the PAN, and it is synchronized with the master. When the master leaves the PAN, the sub-master assumes the master role and a new sub-master is elected. The sub-master is invisible from the slaves viewpoint; only the master is aware of its presence. When the sub-master leaves the network the master nominates a new sub-master; this modification is transparent to the slaves, except to the one that becomes elected sub-master. If, for some reason, two or more devices become disconnect from the PAN they may form a second PAN and elect a master and a sub-master for it. Later on, if the two PANs come together the masters have to decide who will take the master role in the merged network; this specific issue needs further investigation, however.

4.3 Advertisement and Discovery

Advertisement and discovery in ASPAN is based, as much as possible, on legacy mechanisms such as those available in WLAN or Bluetooth. When all the devices share the same link layer technology the legacy mechanisms are enough. In multi-technology scenarios not all the devices can discover the others by just sending and listening to beacon frames. ASPAN defines a new relay mechanism implemented in the BCM, which makes a device to notify the master when it detects a new device in the neighborhood. When a PAN slave discovers a new device in the neighborhood, it first waits for the new device to send the request to join the PAN. Then, the slave relays the message towards the master. For technologies that do not have built-in advertisement and discovery mechanisms, such as Ethernet, ASPAN provides this functionality; in this case, the abstraction module shown in

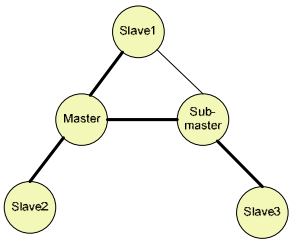

Fig. 3. Connectivity graph maintained by the PAN master

Fig. 2 emulates the beaconing mechanism employed in WLAN or Bluetooth, which consists of periodic messages that include the identification string of the current device. Fully Qualified Domain Names (FQDNs) syntax is employed (e.g. *laptop.BobsPAN.*, *PDA.BobsPAN.*), either when the legacy layer 2 advertisement/discovery or the ASPAN mechanism is used.

4.4 Security

Concerning the protection of a PAN against malicious nodes that may try to join it without authorization, ASPAN specifies a pre-shared key based mechanism, which enables both authentication and authorization of devices willing to join a PAN. The same pre-shared key (K_{PSK}) is also used to encrypt the signaling messages exchanged between PAN devices during the creation of the PAN or between the master and a new joining device until the latter is informed about the current K_{TEK} (see below). K_{PSK} is derived from the password provided by the user when she identifies the devices belonging to her PAN (see Subsection 4.8). The creation of a pre-shared key from such password is performed by applying a Key Derivation Function (KDF), e.g., the KDF specified in [2].

In order to avoid the overuse of the pre-shared for encryption purposes, a temporary encryption key (K_{TEK}) is derived. At the beginning, either when the PAN is being bootstrapped or when some device is joining it, K_{PSK} is used to encrypt the signaling information. Afterwards, the temporary encryption key is used instead; the master is in charge of generating this key for the whole PAN. K_{TEK} is periodically changed so that it becomes harder for an attacker to discover what the content of the control information is; the specific period upon which the master must derive a new key is configurable. The master must notify the slaves about the new K_{TEK} and encrypt it using K_{PSK}.

4.5 Joining Mechanism

When a new device wants to join the PAN, it firstly discovers the device(s) of the PAN in the neighborhood by using the mechanisms defined in Subsection 4.3. After detecting the presence of one or more PAN devices, the joining device broadcasts a BCP JOIN message requesting to join the PAN, and the master device replies to this; the BCP JOIN message is encrypted using the pre-shared key K_{PSK}. When the joining device connects to the PAN through one of the links the master uses, the JOIN message is immediately received by the latter; however, when it connects through a PAN slave, the relay mechanism mentioned in Subsection 4.3 is used. After getting a reply from the master, which is also encrypted with K_{PSK}, the joining device learns the IP version and autoconfiguration framework to use for configuring the PAN scope and the global IP addresses (see Subsection 4.7), the PAN gateway towards the Internet, the PAN device to which it shall send the subsequent signaling messages destined to the master, and the temporary encryption key K_{TEK}. After the new node joins the PAN, the master updates the connectivity graph and the joining node notifies the master, by using the ACP protocol, about the network accesses it can provide to the PAN. Afterwards, the master checks against the user-defined policies whether the (or one of the) access(es) is better than the current one. If this is the case, reconfigurations within the PAN are required with respect to the PAN gateway towards the Internet.

4.6 Leaving Mechanism

The leaving mechanism uses the control tree shown in Fig. 3. When the PAN is composed by devices connected to the same link, things become simple, because all the devices are aware of the others' presence. However, in multi-technology scenarios the control tree of Fig. 3 is needed. Hence, in ASPAN, the master polls the slaves by proactively broadcasting an ARE_YOU_THERE message through the control tree; this message is then re-broadcasted by each slave until the leaf PAN slaves are reached (e.g., *Slave1* in Fig. 3). Next, each slave still connected to the PAN sends an ACK towards its parent node which, in turn, after receiving all ACKs from its child nodes, sends a message to its parent node that contains its information and the information related to its child nodes. This process is repeated until the information reaches the master; the master receives a single ACK for each branch of the control tree. In this way the master is able to detect when a slave suddenly leaves the PAN; a gently leaving procedure is also defined, where the leaving device sends an I_AM_LEAVING message towards the master.

If the leaving device is the master, the sub-master becomes master and a new sub-master is elected; if the sub-master leaves the PAN instead, a new sub-master is elected, but the PAN can still operate without any change from the slaves point of view. The election of the new sub-master is performed by the master as it possesses all the information required for that. If the leaving device is the current PAN gateway, a new gateway is selected by the master taking into account the user-defined policies. After the new gateway is selected, the master notifies the slaves accordingly. In turn, slaves update their default gateway information concerning the new selected gateway; in addition, since the new PoA may support a different IP version, slaves may have to enable the proper IP stack and configure their internal routing tables accordingly. The mechanism used to perform such reconfigurations depends on the network configuration used within the PAN (see Subsection 4.7).

4.7 Network Configuration

When the PAN devices are forming the PAN, or a new device is joining it, the proper IP version and autoconfiguration mechanism have to be negotiated/informed. Afterwards, the configuration of an IP address for intra-PAN communication, so-called PAN scope address, is performed; this approach guarantees stability with respect to IP connectivity within the PAN, since such IP address is maintained independently of potential changes in the PoA of the PAN. However, in order to acquire external access through the current PAN gateway, for IPv6 each device dynamically configures a global address; for IPv4, the PAN scope address can still be used as the PAN gateway performs NAT. The configuration of both PAN scope and global scope addresses depends on the PAN logical topology. If the PAN devices are all

connected to the same logical link, the traditional IP autoconfiguration mechanisms (e.g., DHCP) can be used; otherwise, the autoconfiguration mechanisms being defined for Mobile Ad-hoc Networks (MANETs) [4] are applied.

In the ASPAN context, and concerning multi-hop scenarios such as the scenario of Fig. 1, the interconnection of the PAN devices can be accomplished by using bridging, routing or both. When bridging is used, all PAN devices become connected to the same logical link, i.e., a single-hop scenario from network layer perspective is created, and traditional IP autoconfiguration mechanisms can be used. The major problem associated to bridging, as widely known, comes up when the number of devices connected to the logical link increases. Thus, ASPAN also supports the use of routing for the same purpose. In that approach the PAN gets divided in multiple logical links instead. In order to maintain connectivity between the PAN devices either an ad-hoc routing protocol [20] or the ASPAN built-in mechanism defined for this purpose can be used; the built-in mechanism applies a centralized model where the master distributes the routing information to each PAN slave every time there is a modification in the topology; using this information the slaves update their internal routing tables accordingly. The third approach is a hybrid one, where the two previous approaches can be used simultaneously.

4.8 User Intervention

ASPAN assumes the following, regarding the end-user intervention:

- The user has to identify explicitly the devices belonging to the PAN; this identification is carried out by assigning them the same PAN ID and password for security reasons;
- The user has to specify the policies governing the attachment of the PAN to the multiple points of attachment it is able to connect to while moving – e.g., WLAN access preferable over UMTS access.

5. CONCLUSION

In this paper we proposed a new framework, the Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which is envisioned to be used in next generation networks environments. These environments are expected to support two IP versions, the corresponding autoconfiguration mechanisms, multiple enabling wireless and wired technologies, and self-management of devices and networks. The proposed solution enables the automatic and dynamic autoconfiguration of a Personal Area Network, and the selection of the best point of attachment towards the Internet according to the network context and user-defined policies.

Currently, an ASPAN prototype for proof-of-concept is being developed and ASPAN evaluation by means of simulations has been started.

6. ACKNOWLEDGEMENT

The authors would like to thank the support from the Portuguese Foundation for Science and Technology (FCT) under the fellowship SFRH/BD/19429/2004/.

7. REFERENCES

[1] B. Cain et al. *Internet Group Management Protocol, Version 3*. RFC 3376, October 2002.

[2] B. Kaliski. PKCS #5: Password-Based Cryptography Specification (Version 2.0). RFC 2898, September 2000.

[3] Bluetooth SIG, *Specification of the Bluetooth System* (version 2.0), November 2004.

[4] C. Bernardos and M. Calderon, *Survey of IP address autoconfiguration mechanisms for MANETs*. Internet Draft, draft-bernardos-manetautoconf-survey-00 (expired), July 2005.

[5] Engelstad, P. E. Towards the Realization of IP-based Personal Area Networks with On-Demand Routing. Ph.D. Thesis, University of Olso, Oslo, 2005.

[6] H. Schulzrinne and R. Hancock. *GIST: General Internet Signaling Transport*. Internet Draft, draft-ietf-nsis-ntlp-09 (work in progress), February 2005.

[7] IEEE 802.15 Working Group for WPAN. http://www.ieee802.org/15.

[8] IST Ambient Networks Project. http://www.ambient-networks.org.

[9] M. Takizawa, et al. MaCC: Supporting Network Formation and Routing in Wireless Personal Area Networks. In *Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)* (Fukuoka, Japan, March 29-31, 2004).

[10] N. Niebert, et al. Ambient Networks: an Architecture for Communication Networks Beyond 3G. IEEE Wireless Communications Magazine, 11 (April 2004), 14-22.

[11] R. Campos and M. Ricardo. Autoconfiguration and Self-management of Personal Area Networks: a New Framework. In *Proceedings of the 15th Meeting of the Wireless World Research Forum* (Paris, France, December 8-9, 2005).

[12] R. Campos and M. Ricardo. Dynamic Autoconfiguration in 4G Networks: Problem Statement and Preliminary Solution. In *Proceedings of the 1st International ACM Workshop on Dynamic Interconnection of Networks (DIN'05)* (Cologne, Germany, September 2, 2005).

[13] R. Droms. *Dynamic Host Configuration Protocol*. RFC 2131, 1997.

[14] R. Droms, et al. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. RFC 3315, July 2003.

[15] R. Wakikawa, et al. *Global connectivity for IPv6 Mobile Ad Hoc Networks*, Internet Draft, draft-wakikawa-manet-globalv6-05 (work in progress), March 2006.

[16] S. Cheshire, et al. *Dynamic Configuration of IPv4 Link-Local Addresses*. RFC 3927, May 2005.

[17] S. Thomson, et al. *IPv6 Stateless Address Autoconfiguration*. RFC 2462, December 1998.

[18] T. Chown, et al. *DHCP: IPv4 and IPv6 Dual-Stack Issues*. Internet Draft, draft-ietf-dhc-dual-stack-04 (work in progress), October 2005.

[19] T. Narten, et al. *Neighbor Discovery for IP Version 6 (IPv6)*. RFC 2461, December 1998.

[20] T. Wysocki et al. A Review of Routing Protocols for Mobile Ad Hoc Networks, Elsevier, 2, 1 (January 2004), 1-22.